Key Findings from

THE INFLUENCE OF SECURITY RISK MANAGEMENT

Understanding Security's Corporate Sphere of Risk Influence

Funded by

ASIS FOUNDATION

FINDING TWO:

SECURITY RISK CONCERNS HAVE LIMITED STRATEGIC IMPLICATIONS

The study found that corporate risks considered by and under the influence of executives with broader influence than security have a higher potential impact at the strategic levels of the organization, as do risks with a higher dread factor. Executives often see security as focused on the operational levels of risk impact. This means security professionals have less influence across broader corporate decision making, and places security lower in the organizational and risk hierarchy than other areas of risk concern. For security to have stronger weighting in their risk message they must communicate how security events impact the strategic objectives of the organization.

The existence and practical application of different types of risk within an organization is acknowledged in various professional standards, including the ASIS International Risk Assessment Standard. However, there is limited articulation or understanding of a hierarchical application of risk within an organization across security texts. Notwithstanding this gap, governmental bodies have formally recognised the existence and importance of a risk hierarchy in the practical application and management of their security risks. For example, following the events of September 11, 2001, the United Kingdom Government commissioned a report investigating how to improve their security and general risk management processes. This report found that the government was required to manage risk at three distinct levels:

- Strategic
- Program (including procurement, establishing projects, and business continuity)
- Operational (including technical issues and managing resources)

Consequently, guidelines were formally published that led a codified stratum or hierarchy of risk under the guise of The OCEG Orange Book guidelines. The acceptance of this hierarchy of risk is also found in the National Institutes of Standards and Technology (NIST) Risk Management Framework used by the U.S. government in identifying information technology risks.

A critical review of the security risk management and risk management standards literature highlighted a disconnect between the expected risk influence of corporate security risk management and the broader corporate landscape. For example, ASIS International defines security risk management as having an "enterprise-wide strategic" role within the organization. Yet, in contrast, the NIST Standard and OCEG Orange Book specifically denoted that this is not the case given the specialist and operational focussed nature of security risk. Such a functional and cultural organizational disconnect was subtly recognised by Briggs and Edwards in their book, *Business of Resilience: Corporate Security for the 21st Century:*

> *"The impact of the security department is proportionate to its ability to persuade individuals and teams all over the company to collaborate and cooperate…formal security training can tend to be risk averse, while businesses need to take calculated risks to stay ahead of competitors."*

The study found this disconnect translated into a practical lack of understanding of the existence of a risk hierarchy (or taxonomy); many of those interviewed during the ASIS Foundation study were unaware of or unable to articulate a hierarchy of risk beyond that of physical security versus cybersecurity.

Participants who saw cyber risk as being more important believed this to be due to cyber event impacts having potential strategic consequences, whereas a security incident is rarely believed to have a strategic impact. This factor was a key point of discussion, with several participants advocating that security risk is often entwined with strategic risks, but this is poorly understood. Such a view highlighted an opportunity to ensure that security risk is better communicated in terms of its strategic impact. The majority of corporate security managers reported that after compliance, cyber was hierarchically more important. This led to an important point being raised by nonsecurity executives and consultants (and those participants who had started in a security role but progressed to nonsecurity/risk/executive roles), that this response in itself highlights how siloed the security professional can be; stating that security managers are missing the bigger picture of enterprise risk across the entire organizational spectrum.

The themes which emerged included the view that security risk is treated as an operational risk rather than one of strategic significance. Furthermore, a risk hierarchy exists within organizations, and this is poorly understood or articulated, resulting in missed opportunities and further disconnect, ultimately leading to reduced security influence amongst organizational decision makers.

Funded by ASIS FOUNDATION

This is part of a series of nine short synopses, this paper explores the findings of an ASIS Foundation study conducted by Dr. Michael Coole, Nicola Lockhart and Jennifer Medbury of Edith Cowan University in Australia in 2022.

The ASIS Foundation, an affiliate of ASIS International, helps security professionals achieve their career goals with certification scholarships, practical research, member hardship grants, and more. The Foundation is supported by generous donations from ASIS members, chapters and organizations. Online at www.asisfoundation.org.